Nach dem Sicherheitspaket ist vor dem Sicherheitspaket

Florian Lehne-Gonzalez 2020-01-06T12:59:37

Der österreichische Verfassungsgerichtshof (VfGH) hat am 11.12.2019 mündlich die Aufhebung unterschiedlicher Maßnahmen des sogenannten Sicherheitspakets der vergangenen ÖVP-FPÖ Regierung verkündet und dazu am 23.12.2019 die 160 Seiten starke Schriftfassung veröffentlicht. Obwohl im Lichte der vorweihnachtlichen VfGH-Erkenntnisse fraglich ist, inwiefern die österreichische Verfassungsrechtslage überhaupt Raum für entsprechende Maßnahmen belässt, scheint die neue türkis-grüne Regierung nun eine Neuauflage der einkassierten Regelungen zu planen. Dies wirft die Frage auf, inwiefern die Koalitionspartner eine verfassungswidrige Regelung zumindest in Kauf nehmen und darauf hoffen, dass der Gerichtshof es am Ende schon wieder richten wird.

Zwischen „subjektivem Sicherheitsempfinden“ und dem „Ende des Rechtsstaats“

Die ÖVP hatte das „Sicherheitspaket“ samt einer umfassenden Überwachung verschlüsselter Nachrichtenkommunikation mittels Bundestrojaner schon im Sommer 2017 gefordert. Damals war sie allerdings noch Juniorpartner in einer großen Koalition mit der SPÖ, die sich dagegen sperrte, wie auch alle anderen zur damaligen Zeit im Nationalrat vertretenen Parteien. Besonders heftig hatten die Grünen das ÖVP-Vorhaben kritisiert, die vor Sicherheitspopulismus warnten, ebenso wie die FPÖ, deren damaliger Generalsekretär Herbert Kickl gar von DDR 4.0 und dem Ende des Rechtsstaats sprach, sollte eine solches Gesetzespaket den Nationalrat passieren.

Wenige Monate später, im Februar 2018, verabschiedete die designierte türkis-blaue Koalition dann das Sicherheitspaket. Der damalige Innenminister Kickl sprach von einer Erhöhung des subjektiven Sicherheitsempfindens in der Bevölkerung und gab die Entwicklung des Bundestrojaners in Auftrag, der bis 2020 geheim fertig entwickelt hätte werden sollen. Daneben dehnte das Sicherheitspaket die Videoüberwachung von öffentlichen Plätzen wie Flughäfen und Bahnhöfen aus, lockerte das Briefgeheimnis erheblich, verpflichtete Erwerber*innen von SIM-Karten zur Registrierung, brachte die Anordnungsbefugnis zum Speichern von personenbezogenen Daten durch Netzbetreiber bis zu längsten zwölf Monaten (Quick Freeze) und baute die Videoüberwachung im Straßenverkehr erheblich aus. Gegen die letztgenannte Maßnahme sowie gegen die Befugnis zur Überwachung verschlüsselter Nachrichtenkommunikation durch „Installation eines Programms in einem Computersystem“ erhoben 61 Nationalratsabgeordnete von SPÖ und Neos und 21 Bundesratsabgeordnete der SPÖ jeweils Antrag auf abstrakte Normenkontrolle durch den VfGH gem. Art. 140 Abs. 1 Z. 2

Bundesverfassungsgesetz (B-VG). Die Antragsteller*innen behaupteten, die einschlägigen Bestimmungen des § 135a Strafprozessordnung (StPO), § 54 Abs. 4b Sicherheitspolizeigesetz (SPG) und § 98a Abs. 2 Straßenverkehrsordnung (StVO) wären mit dem Recht auf Privat- und Familienleben, dem Recht auf Datenschutz, dem Fernmeldegeheimnis, dem Hausrecht, dem allgemeinen Gleichheitsgebot sowie dem rechtstaatlichen Bestimmtheitsgebot unvereinbar.

Entsprechend betrifft die Aufhebung durch den VfGH einerseits die kriminalpolizeiliche Überwachung verschlüsselter Nachrichten durch geheim installierte Software und Geräte (Bundestrojaner) und andererseits die (verdeckte) sicherheitspolizeiliche Fahrzeug- und Fahrzeuglenkererfassung mittels Section-Control und/oder anderer bildverarbeitender technischer Einrichtungen.

Digitale Schleierfahndung

Der VfGH hielt die Anträge im Wesentlichen für zulässig und setzte sich inhaltlich zunächst mit der Videoüberwachung im Straßenverkehr auseinander. § 54 Abs. 4b SPG ermächtigte die Sicherheitsbehörden zur verdeckten Verarbeitung von Fahrzeug- und Fahrzeuglenkerdaten mit Hilfe von „bildverarbeitenden technischen Einrichtungen“ „für Zwecke der Fahndung“. Der Gerichtshof schloss sich den Antragsteller*innen an, die eine Verletzung des Rechts auf Geheimhaltung personenbezogener Daten (§ 1 Datenschutzgesetz, DSG) und des Rechts auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) behaupteten. Weder die Befassung eines Rechtsschutzbeauftragten noch, dass die erfassten (Bild-)Daten nach § 54 Abs. 4b SPG nach längstens zwei Wochen zu löschen waren, konnte den VfGH von der Verhältnismäßigkeit dieser Maßnahme überzeugen. Nach Ansicht des Gerichtshofs ermächtigte § 54 Abs. 4b SPG die Sicherheitsbehörden dazu, Kfz- und Kfz-Lenkerdaten anlasslos und automatisch zu erfassen. Diese Befugnis hatte der Gesetzgeber weder durch eine abschließende Aufzählung der zu erhebenden Daten noch zeitlich, räumlich, instrumentell – auch Gesichtserkennungsgeräte wären für den VfGH darunter subsumierbar – oder durch genauere Beschreibung des Zwecks ausreichend eingegrenzt. Für den Gerichtshof war ausschlaggebend, dass die Verknüpfung der Daten, „welche Personen miteinander unterwegs sind und wer an bestimmten Veranstaltungen teilnimmt […] Aufschluss über das Bewegungsverhalten und die persönlichen Vorlieben einer Person geben kann“. Betroffene müssten überdies die Möglichkeit haben, die gewonnen Daten zu überschauen und kontrollieren, umso mehr als die Überwachung in der Regel nicht von ihrem Verhalten abhängig sei. Ein daraus resultierendes „Gefühl der Überwachung“ könne, so der Gerichtshof, „wiederum Rückwirkung auf die freie Ausübung anderer Grundrechte – etwa der Versammlungs- oder Meinungsäußerungsfreiheit“ haben. Insgesamt sah der VfGH in der Verkehrsüberwachung einen „gravierenden Eingriff“ in § 1 DSG und Art. 8 EMRK und hob aus diesen Gründen auch die sicherheitsbehördliche Anordnungsbefugnis nach § 98a Abs. 2 StVO auf, Section-Control-Anlagen zur sicherheitspolizeilichen Gefahrenabwehr “umzufunktionieren“.

„Mein Haus, mein Computer, meine Privatsphäre“

Im zweiten Teil der Entscheidung beschäftigte sich der Gerichtshof mit der (mangelnden) Verfassungskonformität von § 135a StPO. Diese Norm ermächtigte die Strafverfolgungsbehörden dazu, bereits bei Verdacht auf leichte Vorsatzdelikte verschlüsselte Nachrichten durch „Installation eines Programms in einem Computersystem“ verdeckt zu überwachen. Der Gerichtshof vertrat die Auffassung, dass die vertrauliche Nutzung von Computersystemen und digitalen Nachrichten ein wesentlicher Bestandteil des Rechts auf Achtung des Privatlebens nach Art. 8 EMRK ist. Persönliche Nutzerinformationen würden „Einblicke in sämtliche – auch höchstpersönliche – Lebensbereiche“ ermöglichen und „Rückschlüsse auf die Gedanken des Nutzers, insbesondere Vorlieben, Neigungen, Orientierung und Gesinnung“ zulassen. Eine Überwachung verschlüsselter Nachrichtenkommunikation ist für den Gerichtshof dementsprechend „nur in äußerst engen Grenzen zum Schutz gewichtiger Rechtsgüter zulässig“. Aus diesem Grund ist „die signifikant erhöhte (Streu-)Breite“ des § 135a Abs. 1 StPO schon deshalb unverhältnismäßig, weil sie sämtliche Nutzer eines Computersystems und damit eine Vielzahl von unbeteiligten Personen erfasst. Darüber hinaus gibt es für den VfGH schlichtweg kein schwerwiegendes öffentliches Eingriffsinteresse, das es rechtfertigen würde, bei Verdacht von leichten Vorsatzstraftaten verdeckt verschlüsselte Nachrichten zu überwachen.

Damit im Zusammenhang steht die Ermächtigung gem. § 135a Abs. 3 StPO „zum Eindringen in eine bestimmte Wohnung […], der Durchsuchung von Behältnissen und der Überwindung spezifischer Sicherheitsvorkehrungen zum Zweck der der Installation des Programms zur Überwachung verschlüsselter Nachrichten in einem Computersystem“, die der VfGH jedoch gesondert prüfte und ebenfalls aufhob. Die Maßnahme stellte für ihn eine Verletzung des ältesten (geltenden) Grundrechts in Österreich dar: des Hausrechts, das seit Einführung des gleichnamigen Gesetzes vom 27. Oktober 1862 geschützt ist. Der Schutzbereich dieses Grundrechts sei „im weitesten Sinn“ auszulegen und soll laut der Rechtsprechung, die der VfGH heranzieht, Eingriffe „in den Lebenskreis des Wohnungsinhabers“ verhindern, welche „die persönliche Würde und Unabhängigkeit“ verletzen. Hausdurchsuchungen lässt er vor allem nur dann zu, wenn eine entsprechende richterliche Genehmigung vorliegt, die überdies innerhalb von 24 Stunden dem betroffenen Wohnungsinhaber zuzustellen ist. Der in Rede stehende § 135a Abs.3 StPO ermächtigte nach Ansicht des VfGH aber zur Hausdurchsuchung ohne richterlichen Hausdurchsuchungsbefehl, da es sich bei der Überwachung verschlüsselter Kommunikation und der Installation von entsprechendem Überwachungsgerät laut Bundesregierung eben um eine geheime Maßnahme handele. Der Gerichtshof konnte dieser Argumentation angesichts der Vorgaben des Hausrechtsgesetzes und dessen systematischer Umsetzung in den Hausdurchsuchungsbestimmungen der StPO jedoch nicht folgen.

Die Verfassungswidrigkeit in Kauf nehmen?

Insgesamt ist bemerkenswert, wie dezidiert sich der VfGH zum Schutz der Privatsphäre bekennt, der im Liberalismus gründet und den die österreichische Verfassung mittlerweile durch unterschiedliche Bestimmungen und Dokumente absichert und wie er diesen Schutz in die digitale Gegenwart übersetzt. Der Verfassungsgerichtshof dürfte dabei den Antwortcharakter der unterschiedlichen Bestimmungen im Blick haben, die die Privatsphäre vor unterschiedlich gearteter staatlicher Überwachung schützen sollen, ungeachtet der Epoche und Stand der Technik. Im Zusammenwirken dieser Bestimmungen spannt die österreichische Verfassung gegenüber staatlichen Eingriffen ein verhältnismäßig engmaschiges Netz um die Privatsphäre des Einzelnen, durch das auch für den demokratisch legitimierten Gesetzgeber kaum ein Durchkommen ist und schon gar nicht mit Breitbandüberwachungsbefugnissen wie sie das Sicherheitspaket enthalten hat.

Die verfassungsgerichtliche Beseitigung türkis-blauer „Altlasten“ hat – wie die Aufhebung der Sozialhilfe – die Koalitionsverhandlungen zwischen der ÖVP und den Grünen wohl erleichtert, schließlich hatten die Grünen das Sicherheitspaket bis dato heftig kritisiert. Umso erstaunlicher ist es, dass im vorgestern erschienenen türkis-grünen Regierungsprogramm von einer „verfassungskonformen Regelung zur Überwachung unter anderem für verschlüsselte Nachrichten“ die Rede ist, die auch die Entscheidung des VfGH vom Dezember 2019 berücksichtigen soll. Es ist nicht auszuschließen, dass eine solche Regelung den Bundestrojaner (und die Verkehrsüberwachung) reaktivieren soll. Es ist auch nicht klar, ob sich die Grünen darauf eingelassen haben, weil sie damit rechnen, dass der Verfassungsgerichtshof einen entsprechenden Beschluss ohnehin wieder aufheben würde (zur ebenfalls im Regierungsprogramm enthaltenen und verfassungsrechtlich problematischen Sicherungshaft hier). Eine solche bedingt vorsätzlich verfassungswidrige Gesetzgebung sollte jedoch nicht die etwaigen hohen politischen Kosten und vor allem die Kosten für das Ansehen eines Verfassungsgerichts unterschätzen.
